GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Verifica preliminare. Installazione di un sistema di videosorveglianza - 22 febbraio 2018 [8235119]

[doc. web n. 8235119]

**Verifica preliminare. Installazione di un sistema di videosorveglianza - 22 febbraio 2018**

Registro dei provvedimenti
n. 102 del 22 febbraio 2018

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti, e del dott. Giuseppe Busia, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da XX S.r.l. ai sensi dell´art. 17 del d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice");

Visto il provvedimento generale in materia di videosorveglianza dell´8 aprile 2010 (pubblicato in G.U. n. 99 del 29 aprile 2010, e reperibile sul sito istituzionale dell´Autorità, www.garanteprivacy.it, doc. web n. 1712680), con particolare riferimento ai punti 3.2. e 3.4;

Esaminata la documentazione acquisita agli atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell´art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

**PREMESSO**

**1. L´istanza della società.**

In data 10 maggio 2017, XX S.r.l. ha presentato un´istanza di verifica preliminare (art. 17 del Codice) al fine di istallare un impianto di videosorveglianza cd. intelligente presso un Data Center della stessa Società, sito a XX (XX), Via XX s.n.c. e di prevedere la conservazione delle relative immagini per un tempo superiore ai sette giorni.

XX S.r.l., operante nell´ambito dell´attività di studio, progettazione e assistenza nel settore dei sistemi informatici e telematici, fa parte del gruppo facente capo a XX International, (società nata dalla partnership tra l´azienda statunitense XX e XX), che detiene i diritti esclusivi per la progettazione e realizzazione dei data center XX al di fuori degli Stati Uniti. Al riguardo, è stato riferito che il data Center di XX è realizzato con l´obiettivo di ospitare apparati informatici di aziende o pubbliche amministrazioni, effettuando per i clienti un lavoro di archiviazione, gestione e messa in sicurezza di dati, di informazioni e di "contenuti fondamentali per la continuità dello svolgimento delle attività quotidiane" degli stessi.

Al riguardo, la Società ha altresì aggiunto di dover garantire ai propri clienti la massima protezione rispetto a possibili appropriazioni illecite di dati, all´effettuazione di sabotaggi, nonché ad attività di spionaggio industriale.

Il Data Center, ubicato in una zona industriale, separato dal centro abitato e dislocato su una superficie di ampie dimensioni, è

stato progettato "per offrire sistemi di protezione [...] di altissimo livello al fine di garantire l´integrità della struttura e la continuità operativa" in caso di qualsiasi tipo di criticità, sia essa derivante da eventi accidentali che intenzionali.

Stante l´elevato valore delle strumentazioni ed informazioni che saranno ospitate all´interno del predetto Data Center ed al fine di garantire in ogni occasione la continuità del servizio, oltre all´installazione degli impianti antincendio e dell´allarme antintrusione, la Società ha implementato ulteriori impianti di sicurezza a protezione del personale e dei beni materiali ed immateriali.

Pertanto, proprio nell´ottica di garantire un sistema di sicurezza elevato, la Società ha scelto di dotarsi di un impianto di videosorveglianza cd."intelligente", in grado di riprendere sia il perimetro, sia gli ingressi della struttura, sia gli ambienti interni.

L´impianto, la cui finalità è diretta al solo scopo di tutela del patrimonio, delle persone e dei dati ospitati all´interno del sito anche in relazione a possibili azioni di sabotaggio, nonché ad "attacchi terroristici", verrebbe dotato di un software Video Analytics che permetterebbe, "grazie all´attivazione di vari allarmi, di poter riscontrare nell´immediato evidenti anomalie o possibili comportamenti illeciti nonché contestualmente di poter intervenire prevenendo o limitando eventuali danni".

E´ stato poi specificato che, al fine di rendere veramente efficace il sistema di videosorveglianza, sarebbe necessario poter contare sulla conservazione delle relative immagini per un periodo maggiore di una settimana. Ciò, in considerazione del fatto che, oltre ad una funzione di deterrenza, l´impianto avrebbe il ruolo fondamentale di verificare comportamenti sospetti da parte di soggetti che, in una fase antecedente ad un evento criminoso, abbiano ad effettuare "attività di sopralluogo, studio dello stabilimento e delle misure di sicurezza utilizzate, accesso legittimo o illegittimo ai macchinari" e/o ogni altra attività propedeutica all´eventuale illecito (cfr. nota datata 4 maggio 2017).

Al riguardo, XX S.r.l. ha aggiunto che la necessità di estendere i tempi di conservazione delle immagini sarebbe connessa, oltre che con l´esigenza di rafforzare il livello di tutela delle proprietà aziendali e di garantire la sicurezza dei lavoratori e dei servizi resi alla clientela, anche con la necessità di rispettare gli ulteriori parametri fissati dagli standard di sicurezza PCI-DSS, specifici del settore finanziario. Tale decisione originerebbe dalla duplice esigenza di avere l´opportunità di estendere il proprio portafoglio clienti a società appartenenti al settore finanziario, nonché di doversi adeguare agli standard di sicurezza già implementati dalla Società madre americana "SWITCH", che ospiterebbe al proprio interno dati appartenenti a società e/o banche operanti in tale ambito (cfr. nota del 22 settembre 2017).

In particolare, è stato riferito che tra le misure di sicurezza richieste dai suddetti standard, figurerebbe anche la conservazione delle immagini registrate dai sistemi di videosorveglianza per un arco temporale di almeno 90 giorni (periodo di tempo per il quale si chiederebbe appunto l´autorizzazione al Garante).

A corredo della propria istanza la Società ha affermato:

- di aver conseguito sia la certificazione ISO 9001, standard di riferimento internazionalmente riconosciuto per la gestione della qualità e perciò anche della sicurezza, sia ISO 27001, considerato lo standard internazionale principale per quanto riguarda i sistemi di gestione della sicurezza informatica;

- di aver provveduto ad espletare le procedure previste dalla normativa in materia di controllo a distanza dei lavoratori presso l´Ispettorato territoriale del lavoro di Pavia, ottenendo il provvedimento autorizzativo ad hoc.

**2. Le modalità di funzionamento del sistema**

L´impianto di videosorveglianza che la Società vuole implementare fa parte di un più ampio apparato di sicurezza predisposto a protezione del sito che, oltre alla presenza di Guardie particolari giurate (autorizzate ex art. 133 TULPS), appartenenti alla stessa Società, o anche dipendenti da Istituti di Vigilanza, include un sistema di controllo degli accessi e controllo antincendio, un sistema di "check" documentale, un rilevatore di esplosivo per merci in ingresso, nonché porte e infissi blindati.

L´impianto si avvale di 150 telecamere, dislocate sia all´interno che all´esterno del Data Center, attive 24 ore su 24. In particolare è stato riferito che le apparecchiature esterne sono posizionate in modo da riprendere esclusivamente aree di pertinenza della Società (tra cui parcheggi e passi carrabili - cfr. nota del 10 novembre 2017).

Per ciò che riguarda l´utilizzo del predetto software Video Analytics, è stato riferito che l´applicazione si avvale di differenti

funzionalità di video-analisi, tra cui in particolare, quella di poter rilevare la direzione di un determinato movimento (Directional motion), ma anche di identificare persone e veicoli attraverso la funzione Adoptive motion, di inviare un segnale di allarme allorché un oggetto venga rimosso (Object removal), di rilevare determinati movimenti al di fuori di specifiche direzioni (Object counting) facendo scattare meccanismi di allarme. A completamento del sistema, sarebbe impiegata anche la funzionalità specifica per rilevare il sabotaggio di telecamere (Camera sabotage). Altre funzioni individuate sarebbero relative, invece, all´identificazione di un determinato oggetto, nel momento in cui risultasse fermo all´interno di una specifica area (Abandoned object), alla verifica di comportamenti sospetti da parte di persone o veicoli in specifici contesti predefiniti (Loitering detection), all´individuazione di veicoli fermi in prossimità di zone sensibili definite (Stopped vehicle).

Circa le misure di sicurezza (artt. 31 e ss. del Codice), è stato dichiarato che il videoregistratore sarebbe ubicato in apposito armadio chiuso a chiave in una delle aree tecniche del data Center, con accesso riservato ai soli appartenenti al dipartimento Sicurezza, specificatamente autorizzati e muniti di badge e di specifiche credenziali personali. I monitor preposti alla visione in "real time" sarebbero, invece, collocati in un locale dedicato (SE.COM) e accessibili, solo tramite autenticazione, a soggetti anch´essi designati incaricati del trattamento.

I sistemi di videoregistrazione sarebbero programmati per effettuare la cancellazione automatica dei dati allo scadere del termine, con modalità tali da non rendere più riutilizzabili i dati cancellati.

Per quanto concerne l´obbligo di cui all´art. 13 del Codice di rendere l´informativa, XX S.r.l. ha specificato di aver affisso dei cartelli in prossimità delle aree videosorvegliate, aggiungendo di rendere disponibile, su richiesta, un´informativa più estesa.

**3. Le valutazioni dell´Autorità.**

L´odierna richiesta relativa all´utilizzo del sistema di videosorveglianza sopra descritto, deve essere valutata alla luce dei principi di necessità, finalità, proporzionalità e correttezza posti dal Codice (artt. 3 e 11 del Codice), espressamente richiamati anche nel Provvedimento generale in materia di videosorveglianza dell´8 aprile 2010.

In particolare, per ciò che riguarda l´implementazione del sistema cd. intelligente sopra descritto, secondo tale provvedimento "in linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell´interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi" posti dai citati artt. 3 e 11 del Codice.

In ragione di ciò, si ritiene che sia importante tenere in debito conto la finalità sottesa all´istallazione del predetto sistema, consistente non solamente nell´esigenza di tutela del patrimonio aziendale, ma anche nella tutela del personale e dei dati dei clienti da possibili azioni di sabotaggio e da possibili "attacchi terroristici". In proposito, data l´estrema delicatezza dei servizi gestiti all´interno del Data Center e l´elevatissimo valore della strumentazione in esso contenuta, una loro eventuale manomissione potrebbe non solo arrecare grave danno al patrimonio aziendale, ma sarebbe anche in grado di mettere in pericolo la gestione e la messa in sicurezza di dati, di informazioni e di "contenuti fondamentali per la continuità dello svolgimento delle attività quotidiane" degli stessi clienti. Alcune aree del sito rivestono un ruolo fondamentale per la continuità operativa del Data Center, per cui eventuali condotte illecite, compromettendo l´operatività dei clienti di XX S.r.l., determinerebbero un impatto dannoso anche "su alcune rilevanti attività economiche del nostro Paese".

Tali obiettive circostanze già permettono di ritenere che il sito in questione sia caratterizzato da specificità che giustificano l´adozione di standard di sicurezza di livello superiore alla media. L´implementazione di un sistema come quello sopra descritto avrebbe l´importante funzione di innalzare i livelli di sicurezza del sito.

Per quanto riguarda la richiesta di allungare il termine di conservazione delle immagini videoregistrate, il Provvedimento generale in materia di videosorveglianza dell´8 aprile 2010 prevede che l´allungamento dei tempi di conservazione dei dati oltre i sette giorni, deve essere adeguatamente motivato "con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

Nel caso in questione, la società ha posto a base dell´istanza due distinte esigenze.

In primo luogo, la Società ha dichiarato che una conservazione delle immagini superiore alla settimana e, possibilmente, di alcuni mesi sarebbe finalizzata alla necessità di appurare eventuali condotte criminose e soprattutto di prevenirle, verificando comportamenti sospetti da parte di soggetti che in una fase prodromica effettuassero attività di sopralluogo, di studio dello stabilimento ma anche di rilevazione delle misure di sicurezza utilizzate. Al riguardo, infatti, è stato anche ipotizzato che, visto l´elevato livello di sicurezza comunque presente nel Data Center, un eventuale illecito avrebbe bisogno di un lungo tempo di pianificazione (cfr. nota del 4 maggio 2017), non escludendo peraltro che gli stessi illeciti possano essere anche compiuti da soggetti abilitati ad accedere al Data Center e, quindi, non essere immediatamente riscontrabili (ad esempio, nel caso di copia di dati dai macchinari ospitati dal Data Center).

In secondo luogo, la Società ha aggiunto che la predetta esigenza sarebbe collegata anche alla necessità di adeguarsi ai requisiti di sicurezza PCI-DSS (cfr. definizioni presenti sul sito http://it.pcisecuritystandards.org/minisite/en/about.php), richiesti dalla casa madre, la cui non implementazione determinerebbe una limitazione all´espansione della Società, in relazione alla possibilità di acquisire clienti appartenenti al settore finanziario.

Tali parametri di riferimento internazionale nel campo della sicurezza dei dati relativi ai pagamenti riguardano anche le misure volte a limitare l´accesso fisico ai dati dei titolari di carte di pagamento, anche attraverso l´uso di videocamere per monitorare gli accessi fisici ad aree sensibili (cfr. PCI–DSS –requisiti e procedure di valutazione della sicurezza).

Ad avviso di questa Autorità, all´esito dell´istruttoria sono emersi elementi che inducono a ritenere che, nel rispetto dei principi posti dagli artt. 3 e 11 del Codice, la richiesta della Società, relativa all´installazione di un impianto di videosorveglianza cd. intelligente presso il Data Center in questione, possa essere accolta.

In particolare, l´ubicazione del sito, la sua notevole estensione e l´estrema delicatezza di larga parte delle informazioni ivi custodite, vale a giustificare l´adozione di un sistema di sicurezza di video analisi come quello descritto che, consentendo una rilevazione articolata di eventi sospetti, risulti effettivamente in grado di prevenire accessi non autorizzati ai luoghi più "sensibili" della struttura e, quindi, di scongiurare –o, quantomeno, di ridurre significativamente- il rischio di condotte criminose e/o di manomissioni dei sistemi informatici, da cui potrebbero derivare anche gravi disservizi.

Parimenti, per ciò che concerne, la richiesta della Società relativa all´allungamento dei tempi di conservazione delle immagini ad avviso di questa Autorità, all´esito dell´istruttoria, sono emersi elementi che inducono a ritenere che tale istanza, limitata ad un periodo di 90 giorni, possa essere conforme ai principi posti dagli artt. 3 e 11 del Codice.

Ciò, alla luce delle dichiarazioni rese (sulla cui veridicità la società ha assunto ogni responsabilità ai sensi dell´art. 168 del Codice) e, segnatamente, delle illustrate modalità di funzionamento dell´impianto, volto a tutelare il patrimonio aziendale, il personale e i dati dei clienti, , potendosi escludere che, dall´impiego del predetto sistema, possano conseguire significative lesioni alla riservatezza degli eventuali soggetti interessati alla rilevazione delle immagini.

Nell´ipotesi in cui XX S.r.l. intendesse poi estendere il sistema di videosorveglianza descritto in premessa, per sopraggiunte esigenze di ampliamento del data center, potrà, negli stessi termini e con le medesime modalità autorizzate con con il presente provvedimento, effettuare analoghi trattamenti senza la necessità di presentare a questa Autorità una nuova richiesta di verifica preliminare, ai sensi dell´art. 17 del Codice.

Si tenga comunque presente che, a decorrere dal 25 maggio 2018, data di applicazione del Regolamento (UE) 2016/679, il titolare del trattamento in ossequio al principio di responsabilizzazione di cui all´art. 24 dovrà valutare autonomamente la conformità del trattamento che intende effettuare alla disciplina vigente, verificando il rispetto di tutti i principi in materia nonché la necessità di effettuare, in particolare, una valutazione di impatto ex art. 35 del citato Regolamento ovvero attivare la consultazione preventiva ai sensi dell´art. 36 del Regolamento medesimo.

**TUTTO CIÒ PREMESSO, IL GARANTE**

ai sensi dell´art. 17 del Codice, a conclusione della verifica preliminare ammette l´utilizzo del sistema di videosorveglianza dotato di software Video Analytics e la conservazione delle relative immagini per un periodo di 90 giorni da parte di XX S.r.l., nelle forme e nei limiti di cui in motivazione

*Roma, 22 febbraio 2018*

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia